Hasse-Minkowski theorem, lec 4:
Quadratic forms with p-adic coefficients

0) Introduction

We now want to investigate quadratic forms

$q(x_1,\dots x_n)=\sum_{i\leq j} q_{ij}x_ix_j$ w. $q_{ij}\in\mathbb{Q}_p$

Here's a motivation. Our original goal in Lec 1 was to investigate quadratic forms with coefficients in $\mathbb{Q}$: we wanted to know when such a form represents 0 (over $\mathbb{Q}$). Thanks to Sec 3.1, we know that $\mathbb{Q}\subset\mathbb{Q}_p$ & so if for q with rational coefficients $q(x_1,\dots x_n)=0$ has a nonzero solution in $\mathbb{Q}^n$, then it (tautologically) has a nonzero solution in $\mathbb{Q}_p^n$ ($\forall p$). This gives us a necessary (but not sufficient) condition for q representing 0 over $\mathbb{Q}$. For example, the 1st exercise in Lec 1 (partly solved in Lec 2) can be stated as:

Example/exercise: $x_1^2-2x_2^2+3x_3^2-6x_4^2$ does not represent 0 in $\mathbb{Q}_3$, while $x_1^2+x_2^2+x_3^2-7x_4^2$ does not represent 0 in $\mathbb{Q}_2$.

The main result of this lecture is:

Theorem: For $n \geq 5$, every quadratic form $q(x_1, \ldots x_n)$ with coefficients in $\mathbb{Q}_p$ represents 0 over $\mathbb{Q}_p$, i.e. $q(x_1, \ldots x_n) = 0$ has a nonzero solution in $\mathbb{Q}_p^n$.

This theorem explains but does not (yet) prove Theorem from Lec 1 (if $q(x_1, \ldots x_n)$ w. $n \geq 5$ & rational coefficients represents 0 over $\mathbb{R}$ then it represents 0 over $\mathbb{Q}$)

1) Recap

Recall that in Lec 1 we worked with quadratic forms w. coefficients in $\mathbb{F}$, which can be $\mathbb{Q}, \mathbb{R}$, or, in fact, $\mathbb{Q}_p$. And:

1) introduced equivalence of forms via invertible linear changes of variables (with coefficients in $\mathbb{F}$)

2) proved that any $q(x_1, \ldots x_n)$ is equivalent to diagonal $q' = \sum_{i=1}^{n} q_i x_i^2$ ($q_i \in \mathbb{F}$). Below we'll use notation $[q_1, \ldots, q_n]$

for this diagonal form. Moreover, if q represents $a \in \mathbb{F} \setminus \{0\}$ then we can find diagonal q' w. $q_1 = a$.

Rem: Two different diagonal forms can be equivalent:

a) Permuting q_i's results in equivalent forms (the corresponding change of variables is a permutation)

b) If $m<n$ & $[q_1, \dots, q_m] \sim [q_1', \dots, q_m']$, then $[q_1, \dots q_n] \sim [q_1', \dots, q_m', q_{m+1}, \dots, q_n]$ ($\forall q_1, \dots q_n, q_1', \dots, q_m' \in \mathbb{F}$) (change only the 1st m variables).

c) $[q_1, \dots, q_n] \sim [a_1^2 q_1, \dots, a_n^2 q_n]$ $\forall a_i \in \mathbb{F} \setminus \{0\}$ (the corresponding change of variables is rescaling the x_i's).

2) Proof of Theorem for $p>2$

If q, q' are equivalent, then q represents 0 if and only if q' does. So we can assume that $q(x_1, \dots x_n) = \sum_{i=1}^{n} q_i x_i^2$ for $q_i \in \mathbb{Q}_p$. If one of q_i is 0, we are done, so we can assume that $q_i \neq 0$ $\forall i$.

Our strategy is as follows: $n \geq 5 \Rightarrow$ at least 3 of q_i's (say (q_1, q_2, q_3)) have orders of the same parity. We'll see (this is a crucial step) that $[q_1, q_2]$ represents $-q_3$. Once this is known we can argue as follows. By 2) above $[q_1, q_2] \sim [-q_3, q_0]$ for some $q_0 \in \mathbb{Q}_p$. Then by 6), we have $[q_1, \dots, q_n] \sim [-q_3, q_0, q_3, \dots q_n]$, which represents 0: plug $x_1 = x_3 = 1$, $x_i = 0$ for $i \neq 1, 3$.

So to prove the theorem it remains to show:

Important lemma: If $\mathrm{ord}(q_1) \equiv \mathrm{ord}(q_2) \bmod 2$, then $[q_1, q_2]$ represents any α w. $\mathrm{ord}(\alpha) \equiv \mathrm{ord}(q_i) \bmod 2$.

Proof: $[q_1, q_2]$ represents $\alpha \Leftrightarrow \exists\, x_1, x_2 \in \mathbb{Q}_p \mid q_1 x_1^2 + q_2 x_2^2 = \alpha$
$\Leftrightarrow z y_1^2 q_1 \cdot (x_1/y_1)^2 + z y_2^2 q_2 (x_2/y_2)^2 = z\alpha \Leftrightarrow [z y_1^2 q_1, z y_2^2 q_2]$ represents $z\alpha$, $\forall z, y_1, y_2 \in \mathbb{Q}_p \setminus \{0\}$. So we can assume that

$$q_1 = 1, \ \mathrm{ord}(q_2) = \mathrm{ord}(\alpha) = 0.$$

In Lemma 1 of Sec 3.2 we've seen that $\sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$ w. $b_0 \neq 0$ is a complete square $\Leftrightarrow b_0$ is a quadratic residue. A more general (but equivalent) claim is:

(*) For $\alpha=\sum_{i=0}^{\infty} a_i p^i$, $\beta=\sum_{i=0}^{\infty} b_i p^i$ $(a_0, b_0 \neq 0)$, α/β is a complete square $\Leftrightarrow$ a_0, b_0 are either both quadratic residues or both quadratic nonresidues.

Write $q_2=\sum_{i=0}^{\infty} b_i p^i$ $(b_0 \neq 0)$. If a_0 is a quadratic residue, we are done: $\alpha = x_1^2$ for suitable x_1. And if b_0, a_0 are both quadratic nonresidues, then we are also done: $\alpha = q_2 x_2^2$. It remains to handle the case when b_0 is a quadratic residue, while a_0 is not.

First, we claim that $\exists$ quadratic non-residue can be presented as the sum of two quadratic residues.

Assume the contrary. Then the subset $X=\{\text{quadratic residues}\} \sqcup \{0\} \subset \mathbb{Z}/p\mathbb{Z}$ is closed under taking sums. This is impossible: the only subsets of $\mathbb{Z}/p\mathbb{Z}$ closed under taking sums are $\varnothing, \{0\}, \mathbb{Z}/p\mathbb{Z}$.

So we can find $y_1, y_2 \in \mathbb{Z}_p$ s.t. $y_1^2 + q_2 y_2^2 = \alpha' = \sum_{i=0}^{\infty} a_i' p^i$, where a_0' is a quadratic non-residue; by (*), $\alpha'/\alpha = y^2 \Rightarrow$ $(y_1/y)^2 + q_2 (y_2/y)^2 = \alpha$. $\square$ of Lemma.

The case of $p=2$ (more complicated) will be handled in a problem set.

3) Hasse-Minkowski theorem

Our goal was to prove that a quadratic form with rational coefficients represents 0 over $\mathbb{Q}$ if it represents 0 over $\mathbb{R}$ provided $n \geq 5$. We have proved something related: that every quadratic form over $\mathbb{Q}_p$ in $n \geq 5$ variables represents 0. At the first glance, this doesn't help much: the implication is that a form representing 0 in $\mathbb{Q}$ represents 0 in $\mathbb{Q}_p$, not the other way around.

Theorem If a form q with rational coefficients represents 0 over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p, then it represents 0 over $\mathbb{Q}$.

Exercise: Prove this for $n=2$.